In the Specification

Applicants propose amending the specification as set forth in the following replacement paragraphs:

At page 1, lines 11-20:

In addition, U.S. patent applications Ser. Nos. ~~09/___,___; and 09/___,___; 09/___,___; and 09/___,___~~ 09/589,496; 09/589,500; 09/589,427; and 09/589,501, respectively entitled (1) "USING ELECTRONIC SECURITY VALUE UNITS TO CONTROL ACCESS TO A RESOURCE"; (2)"UNIFIED MONITORING AND DETECTION OF INTRUSION ATTACKS IN AN ELECTRONIC SYSTEM"; (3)"IDENTIFICATION OF AN ATTACKER IN AN ELECTRONIC SYSTEM"; and (4) "A BANKING INFRASTRUCTURE FOR GENERATING AND MANAGING ACCESS RIGHTS IN AN ELECTRONIC SYSTEM", have all been filed on June 7, 2000 for Yechiam Yemini, Apostolos Dailianas, and Danilo Florissi. The above four applications are assigned to the assignee of the present application. The contents of the above four applications are relevant to the subject matter of the present application and are fully incorporated herein by reference.

At page 5, lines 10-20:

A significant body of research and implementation work has been devoted to protecting individual resources or whole network domains. Two of the most commonly used protection techniques are (1) firewalls/security gateways (see, e.g., Cheswick, and Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker," Addison-Wesley, Reading, Mass. 1994), and (2) a combination of authentication and access control lists (see, e.g., Kaufman, Perlman, and Speciner, "Network Security - Private Communication in a Public World," Prentice Hall series in computer networking and distributed systems, 1995; Kohl and Neuman, "The ~~Kerberos~~ Kerberos® Network Authentication Service (V5), "RFC 1510, Sept. 1993; Needham, FL, and VL ~~Schroeder~~ Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of ACM, Vol. 21, Dec. 1978, pp. 993-999;

and Needham and Schroeder, "Authentication Revisited," Operating Systems Review, Vol. 21 # 1, Jan. 1987).

At page 6, lines 6-12:

Authentication mechanisms, such as the well-known ~~Kerberos, can verifies~~ Kerberos® authentication mechanism, can verify the identity of network entities involved in a transaction. This verification is typically achieved through a certificate generated by a trusted certification authority. Certificates are valid for a period of time during which they authenticate the identities of the entities involved in a transaction. In ~~Kerberors~~the Kerberos® authentication mechanism, "tickets," which are issued as part of the authentication between an entity and a resource it wishes to access, provide the entity with unlimited access to the resource during the validity of the ticket.

At page 6, lines 13-17:

Access control lists (ACLs) determine the authorization of the entity to access the specific resource. An ACL is associated with each resource whose access needs to be restricted. However, ACLs become prohibitively expensive as they increase in size, since they become expensive to store, difficult to maintain, and provide relatively little assistance in isolating attack sources, once the source or sources of an attack ~~has~~ have been identified.

At page 8, lines 7-15:

However, current financial institutions associated with e-commerce do not address certain key issues. For example, the issues of scalability and transparency are not addressed. Rather, most of their work research focuses on centralized infrastructure particular to the associated payment protocol. A second issue not addressed is the protection of the online financial infrastructure itself from intruders (i.e., from attackers). Furthermore, the volume of transactions created by trading both physical resources and higher level services is orders of magnitude larger than that assumed by typical e-cash protocols. Therefore, it becomes imperative to ~~develop:~~ develop protocols with very low overheads in terms ~~of bandwidth;~~ of: bandwidth; information that needs to be stored; and the cost of payment functionality.

At page 9, lines 21 through page 10, line 5:

In an illustrative embodiment of the invention, enhanced protection is provided in order to prevent unauthorized access to resources in an electronic system, such as a network. A component of the system, such as a ~~client~~ client, is allowed access to a resource only in exchange for payment of an appropriate amount of a resource-specific electronic security value unit or currency. For example, to receive access rights, payment from the client is transferred to a resource manager managing the resource. For example, a www browser software needs to pay a www server to access its pages.

At page 12, lines 4-11:

In another embodiment, electronic security value instruments or units are used to protect access by components to internal computer system resources. For example, a ~~Java~~ Java® program executing over a ~~Java~~ Java® Virtual Machine (JVM) is required to pass payments, in electronic security value units, for its usage of CPU time, memory, special application program interfaces (API) provided by the JVM, and access to operating system (OS) resources. The security value instrument is represented by a data structure that is passed to a manager of the JVM who authorizes access and collects payments for these accesses. The resource manager handles access control through pricing and payment.

At page 13, lines 14-20:

Further, in the second aspect, the IDM monitors the ~~resources~~ resource manager or the local bank of the monitored resource to determine a pattern of payments received ~~by~~ by the resource from all clients in any domain. Next, the IDM compares the monitored pattern of payments with a predetermined pattern of payments to determine whether the difference is greater than a predetermined difference. If the difference is greater than the predetermined difference, then the IDM determines that a potential attack has occurred. Subsequently, the IDM analyzes the potential attacker's specific accesses and alerts security administrators to the potential attack.

At page 14, lines 12-17:

In short, the above embodiments detect anomalous behavior by one or more intruders in ~~accessing into~~ accessing a resource of a network to limit the ~~affects~~ effects of an attack by examining patterns of expenditures of electronic security value units in particular time periods. In particular, the above embodiments provide a unified mechanism, measuring access behaviors using electronic security value units, to detect anomalies generated by attacks, regardless of the specific operational details of the clients or resources.

At page 16, lines 12-18:

In a particular illustrative embodiment of the invention, the measure of exposure to an attack on, e.g., a resource in an electronic system, can be quantified and controlled. Similarly, the measure of attack power of, e.g., ~~one or~~ one or more components in an electronic system, can be quantified and controlled. In particular, a price set for a resource is determined in electronic security value units. This is illustratively done by the resource or resource manager. Next, a budget, also in electronic security value units, ~~are determined, by e.g.,~~ is determined by, e.g., a domain or resource manager, and distributed to one or more components, such as to a client.

At page 24, lines 1-2:

Section IV, ~~below, how~~ below, describes how attacks can be detected, e.g., by monitoring payments of electronic security value units.

At page 31, lines –10-13:

In addition, resource manager 12 is also illustratively implemented as a software server, operating on a ~~Java~~ Java® Virtual Machine (JVM) or conventional OS platform. Other examples of the implementation of the resource manager include a hardware server or an application running on the resource (if the client is, e.g., a server) itself.

At page 33, lines 4-8:

The mint bank 24, X exchange bank 18, Y exchange bank 16, and X.c1 domain bank 15 may be implemented as separate software servers, written in C++ and operating on a

Solaris® or ~~Linux ®~~ Linux® platform. Communication between each bank may be encrypted using, e.g., ~~RSA~~ RSA® libraries (for non-commercial use) having public and private keys that are 512 bits long (or of different length), or encrypted using other encryption techniques for commercial use.

At page 36, lines 7-11:

FIG 4, illustrates an example of the information, divided into fields, included in a bill. Of course, it should be appreciated that this is only one example and other fields may be included or omitted, as desired. The bill 60 includes ~~a issuing~~ an issuing domain's exchange bank field 62, a unique ID field 63, an amount field 64, a validity field 65, a new owner's exchange bank field 66, a purpose field 67, a provider field 68, and a timestamp field 69. Each of these fields are described below:

At page 38, lines 15-17:

Step 2: Client manager 14 acting on behalf of ~~client R1~~ client C1 finds the price to access books-on-demand and the type of electronic security value units (currency) accepted by the resource R1 from resource manager 12.

At page 47, lines 10-19:

In an illustrative embodiment of the invention, both the measure of exposure to an attack on, e.g., a resource, as well as the measure of attack power of, e.g., one or more components, can be quantified and controlled. In particular, a price set for a resource, or for each resource in a group of ~~resource,~~ resources, where each resource has its own price, is determined in currency (i.e., electronic security value units). This is illustratively done by the resource or resource manager. Next, a budget is ~~determined, by e.g,~~ determined by, e.g., a domain or resource manager, and the currency is distributed to one or more clients. A measure of exposure to attacks of the resource, as well as a measure of attack power by the ~~components~~ components, can then be ~~determined,~~ determined based on the determined price and on the budget. In addition, access to the resource is controllable, based on either or both of the above measures.

At page 48, lines 5-8:

In short, the risk of attack of a resource, as well as the attack power of a ~~client~~ client, are measurable. Therefore, a client can be denied access to the resource when said risk of attack is above a predetermined threshold. The threshold can be dynamically adjusted, as desired. Accordingly, the resource is protected against attacks.

At page 48, lines 9-11:

~~The below Sections IVb1-3~~ Section IV, parts A-C, below, illustrate additional examples of mechanisms utilized by the resource manager to limit exposure to attacks, ~~namely~~ namely, control of budget allocation, ~~price control,~~ price control, and control of budget expenditure.

At page 49, line 16 through page 50, lines 3:

FIGs 8A and 8B ~~depicts~~ depict two such pricing policies; FIG 8A graphically illustrates a pricing policy that depends on the time during the day when the resource is used and FIG 8B graphically illustrates a pricing policy that depends on the service capacity *C* of a resource that is currently being used by all clients accessing the particular resource. In the time-based pricing policy in FIG 8A, the price of a resource rises and falls based on the time of day when the resource is accessed. Of course, the exact rise and falls are set by the resource. In the capacity-based pricing policy in FIG 8B, the resource manager sharply increases the price to access the resource above a predetermined threshold capacity, Cthres, providing feedback to the clients that the resource is entering ~~in~~ into an undesirable "region of operation." Legal users and attackers will have to pay the increased price to continue accessing the resource.

At page 50, lines 4-7:

In addition, the resource manager can provide access to the resource for a different price to different clients. Differentiated prices can play an important role to security. For example, attackers may see a much higher price than normal clients. This will deplete an ~~attackers~~ attacker's available budget much faster and, in certain cases, prevent the attack.

At page 53, lines 8-12:

Now assume that the X bank transmits bill 80 to client manager 14, who, in ~~turns,~~ turn, transmits bill 80 as payment to resource manager 12 to access resource R1. This transaction establishes the "second association." Specifically, the second association links the particular bill to the access of the particular resource, i.e., R1. The second association may be stored in the client manager 14, in a second association field 84, or anywhere else in the RAL, as desired.

At page 53, line 17 through page 54, line 3:

However, if it is necessary, for example, to prove that a particular client is responsible for a particular access, then the second association should be analyzed. Accordingly, the recorded second association is analyzed to determine which electronic security value units were used to access the resource. Once the actual electronic security value units used by the client are determined, the first association of the actual electronic security value units is analyzed. This first association indicates the client. Therefore, using this powerful feature of the present invention, the attacker is identified and provably linked to a particular attack. In addition, note that the first and second associations are protected against, e.g., unauthorized access, tampering, and duplication. This may be ~~achieve~~ achieved by various protection techniques, such as by encryption.

At page 54, line 13 through page 55, line 5:

As shown in FIG 7, an illustrative banking architecture is hierarchical and distributed. FIG 7 illustrates a more detailed banking hierarchy than the banking hierarchy previously described with reference to FIG 2. In FIG 2, the banking hierarchy included ~~mink~~ mint bank 24, exchange banks 18 and 16 of respective domains X and Y, and domain bank 15 of subdomain X.c1. ~~However,~~ However, in the banking structure of FIG 7, three domains are illustrated, namely U1, U2, and e-Store, as indicated by their respective exchange banks 52, 54 and 56. Each domain is associated with mint bank 42 and with several subdomains (indicated by their domain banks) that preferably have their own currency and currency distribution policies. For example, the U2 currency domain is parent to a currency

subdomain, cs 74 (or U2.cs), which in turn is parent to two additional currency subdomains, "A" 66 and "B" 68 (or U2.cs.A and U2.cs.B). U1 currency domain is parent to currency subdomain, math 72 (or U1.math), and the e-Store currency domain is parent to two subdomains, books 65 and mp3 67. Each of the above subdomains, represented by its corresponding domain bank, may have its own subcurrency and currency distribution policies (i.e., its own electronic security value units and policy for distribution of these units). For example, books 75 and mp3 77 may have the same e-Store currency or may have their own e-Store.books and e-Store.mp3 currency.